METHOD AND SYSTEM FOR DATA ENCRYPTION/DECRYPTION IN A CLIENT-SERVER ARCHITECTURE

REFERENCE TO RELATED APPLICATIONS

The present application claims priority to Taiwan application No. 089122775 entitled " Method and system for data encryption/decryption in a client-server architecture " filed on 27 October 2000.

BACKGROUND OF THE INVENTION

Field of the Invention

This invention generally relates to a system for data encryption/decryption. Through drag-and-drop a decryption icon onto a window interface, the encrypted data is decrypted and displayed in a window provided by the decryption icon.

Description of the Related Art

Internet has become an essential tool to access to information sources nowadays. The sources make available by Internet covers various topics such as science, literature etc., whereas it also contributes to the rapid spread of information concerning violence, pornography, crime-related materials.

Focus on the complication of the Internet resources as mentioned, functions to categorize web content has been added to current web browsing applications to screen unwanted materials for users who requires it. However, due to the fact that configuration for such function in browsing applications is manual and the censorship standards remains a controversial issue, content censor is open to better solutions.

In addition, there are websites using member registrations to differenriate their audience. The method allows web administraters to offer a more comprehensive service, yet it does not serve as an efficient means for content censor. Otherwise, often websites only offer warnings such as "This website contains explicit language and images, adult only".

Furthermore, there is also means to screen unwanted websites by blocking access to the website or specific web pages.

SUMMARY OF THE INVENTION

The invention provides a method and system for data encryption/decryption in a client-server architecture to facilitate censorship of the web content and at the same time to establish a fee-based membership. The invention divides the content to distribute on the Internet into a plurality of channels, then decides which channels should be encrypted. Encryption can either proceed at the server or client. Client is free to choose channels to watch. If the chosen channels are encrypted and as a result unreadable or scramble, then client has to request or purchase a decryption device for channel decryption. As the decryption device is installed in the client computer system. The decryption device is represented as an icon such as a magnifier for the client to drag and drop onto the images of the channels which the client wish to read or watch. It followed that, the decryption device then confirm whether the channels beneath it is the aiming channels. If yes, the device proceed to descrypt channels so that the client can read or watch the corresponding decrypted channels lies beneaththe decryption device. Once the decryption deviceis removed from the channel image, then the content of the channel will be retured to the encrypted state and become unreadable or scramble again.

Moreover, password authentication is available before dragging and dropping the decryption device in order to prevent misuse of the device by a third party.

BRIEF DESCRIPTION OF THE DRAWINGS

The following detailed description, which is given by way of example, and not intended to limit the invention to the embodiments described herein,can best be understood in conjunction with the accompanying drawings,in which:

FIG. 1 illustrates a block diagram illustrating the server according to the present invention;

FIG. 2 illustrates a block diagram illustrating the client according to the present invention;

FIG. 3 illustrates a block diagram illustrating the combination of the server and the client according to the present invention;

FIG. 4 illustrates a user interface from the client in an embodiment according to the present invention;

FIG. 5 illustrates a flowchart of the encryption steps according to the present invention;

FIG. 6 illustrates a flowchart of the encryption/decryption steps according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The embodiment employing the invention discloses a method and system for data encryption/decryption in a client-server architecture. FIG. 1 is a block diagram illustrating data encryption of a server 12 according to the invention. The server 12 includes a data management module13, a channel management module14, an

encryption module15 and a data-transferring module 16. As a plurality of data sources 11 are stored in the data management module 13, The channel management module 14 divides a plurality of data source 11 into a plurality of channels based on the content censorship or fee-purpose. It followed that the encrypted channels 15 then encrypt each channel separatively, which requires different means for decryption to strengthen the control over channels. That can effectively prevent users decrypt all encrypted channels with encryption means of one. After the separative encryption of each channel, the data-transferring module 16 waits for channel request from the client. Upon receiving the requests, the data-transferring module 16 transfers encrypted channel in the form of data stream to the client making the request. Moreover, the encryption module 15 also offers channels without encryption which resulted in a data stream transferred by the data-transferring module16 which may contain both encrypted channels and unencrypted channels.

Referring to FIG. 2, a client31 includes a channel-receiving module 29 and a decryption module 30. When the channel-receiving module 29 receives the data stream at the client 31, the decryption module 30 is required for the decryption. The channel receiving module29 using a data-receiving module 21 to make a channel request, then receive the data stream from the server12. A channel differentiating unit 22 recovers the data stream into a plurality of channels. The channels are temporarily stored in data buffer unit 23. The first interface unit 24 is a window interface, and users can select or flip to different channels with it. However, users can select one channel at one time. The format of the performing window environment follows the format of the channel temporarily stored in a data buffer unit 23. For example, if channel A contains graphics then channel data will performed the graphics it intented to render. In the same way, If

channel B is audio, then the performing of decrypt channel will be audio. If channel C is multimedia format, then the performing of channel C will be multimedia. However, it is restricted to the condition that the channel data temporarily stored in the data buffer unit 23 is unencrypted. Concerning encrypted data, the first interface unit 24 regards it as text files which results in scrambles shown in the window. The channel-receiving module 29 further comprises a first detection unit 25 for receiving encrypted data of the first interface unit 24. It is also responsible for detecting whether there is any other windows lies on top of the window provided by the first interface unit 24. In the same drawing, the first detection unit 25 of the decryption module 30 is used for detecting whether there is a decryption module30 above it when channel performed in the first interface unit 24 has the same decryption key as the decryption module30. If yes, first detection unit 25 will transfer encrypted data to the decryption module30. Similarly, the second detection unit 28 is used to detect wherther a channel-receiving module29 is under itself when the decryption key of decryption module30 is the same with channel performed on the first interface unit24. If yes, the second detection unit 25 then receives the encrypted data from the first detection unit 25. However, after the decryption module30 is removed from the top of the channel-receiving module 29, decryption terminates. Upon second detection unit 25 receiving the encrypted data, decryption unit 26 then proceed to decryption and display decrypted data with the second interface unit 27, The second interface unit 27 is a window interface and determines the window interface executing environment according to the format of the decrypted data. For example, if the data is graphics then it performs graphics, if it is audio then it performs audio and if it is multimedia then it performs multimedia. The display format is loyal to the decrypted data format.

FIG. 3 is a combination of FIG. 1 and FIG. 2. In the FIG. 3, server 12 further comprises a plurality of decryption module 32. In which, the number of the decryption module 32 depends on the numbers of the channel and means of encryption. One decryption module32 corresponds to one channel. The client 31 downloads each decryption module 32. As shown in the drawing, the decryption module 30 is represented as an icon on the screen at the client31. In the FIG. 4 (a), decryption module30 is represented as a magnifier icon, users can drag and drop the decryption module 30 onto the channel-receiving module29 via any input decive shuch as a mouse. The decryption module 30 then determines the window size of the decryption module 30 based on the window size of the channel-receiving module 29. Followed by said decryption means to decrypt and display channel data on the decryption module 30 as shown in the FIG. 4 (b). Provided the decryption module 30 is removed from the channel-receiving module 29, then it returns to the state as shown in the FIG. 4 (a). For strengthening the control over the use of the decryption module 30, a password authentication is available before the drag and drop of the decryption module 30 takes place.

Referring to FIG. 4, the invention further discloses a method for decryption. As in the FIG. 5, in the step51, receiving and storing encrypted data in a window interface. Then in the step 52, the method proceeds to moving a decryption icon onto top layer of the window. At step 53, the control flows to executing decryption. Followed that it moves to step 54 diplaying decrypted channels on the same window provided by the designated icon.

With reference to to FIG. 3, an embodiment according to the invention shown in the FIG. 6 further discloses a method for data encryption/decryption. Server divides data into a plurality of channels, encrypts each channel separatively and generates a

plurality of encrypted channels 62. A client executes step 61 to make a request to a server, followed to receive a data stream of encrypted channels transferred in response to the request from server. In the step 64, client differentiates the data stream into a plurality of encrypted channels, and then the client selects channel K. In the step 65, the client makes a request for channel K to the server and downloads decryption unit K from the server. In step 66, user move decryption unit K onto the top of the selected channel K and generates decrypted data. According to the format of the decrypted data, decryption unit K determines display format and displays decrypted data in the step 67.

In addition, in step 66, moving decryption unit K onto the top of the selected channel K, for strengthening the control over the use of decryption unit K, password authentication is available before the action.

It is thought that method and system for data encryption/decryption in a client-server architecture and many of its attendant advantages will be understood from the foregoing description and it will be apparent to one skilled in the art that various changes may be made in the form, construction and arrangement of the parts thereof without departing from the spirit and scope of the invention or sacrificing all of its material advantages, the form hereinbefore described being merely a preferred or exemplary embodiment thereof. It is clear that other embodiments equivalent to the disclosed preferred embodiments could also be developed using components that may be developed in the future.